AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A processor readable medium encoded with a data structure representing a valued content in a digital form, the data structure comprising:

a preexisting digital file having independent value to a provider; and

a digital string provided by a purchaser in clear form to a provider system of said preexisting digital file, said digital string having a latent value at least to said purchaser, said digital string modified according to a key and embedded two or more times in said preexisting digital file by said provider system, to form an embedded digital file, before the valued content is conveyed to said purchaser, wherein said digital string is embedded at least once in a hidden manner forming a hidden digital string, wherein said provider makes said key publicly available, and wherein said embedded digital file on said processor readable medium is processable by a computer program using ~~only~~ said key to reveal said embedded digital string in clear form.

2. (Previously presented) A processor readable medium in accordance with claim 1, wherein said hidden digital string further comprises said digital string encrypted by said provider system, to form an encrypted digital string, said encrypted digital string embedded in said preexisting digital file.

3. (Previously presented) A processor readable medium in accordance with claim 2, wherein said encrypted digital string further comprises a private digital string encrypted using a public key of a private/public encryption key pair and a public digital string encrypted using a private key of said private/public key encryption key pair.

4. (Previously presented) A processor readable medium in accordance with claim 1, wherein said digital string further comprises said digital string embedded at least once in said preexisting digital file in a human perceptible form.

5. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises a digital watermark generated by said provider system from said digital string.

6. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises a digitized image.

7. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises text.

8. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises video images.

9. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises digitized audio.

10. (Previously presented) A processor readable medium in accordance with claim 1, wherein said latent value further comprises information which places said purchaser at increased financial risk when known by another.

11. (Previously presented) A processor readable medium in accordance with claim 1, wherein said preexisting digital file further comprises a provider digital string.

12. (Previously presented) A processor readable medium in accordance with claim 11, wherein said provider digital string further comprises said provider digital string encrypted by said provider system.

13. (Canceled)

14. (Previously presented) A processor readable medium in accordance with claim 1, further comprising a portable medium having said embedded digital file recorded thereon.

15. (Currently amended) A processor readable medium encoded with a data structure representing a valued content in a digital form, the data structure comprising:

a preexisting digital file having independent value to a provider; and

a digital string provided by a purchaser in clear form to a provider system of said preexisting digital file, said digital string encrypted by the digital processor of said provider system according to a key and combined with an encrypted provider digital string encrypted according to said key to form a combined encrypted digital string, said combined encrypted digital string embedded two or more times in said preexisting digital file by said provider system to form an embedded digital file before the valued content is conveyed to said purchaser, said digital string having a latent value at least to said purchaser which places said purchaser at increased financial risk when known by another, ~~and~~ wherein said embedded digital file is processable by a computer program using said key to reveal said combined encrypted digital string in clear form, and wherein said encrypted provider digital string includes a notice of a reward for detecting that said valued content has been illicitly distributed to other than said purchaser.

16-20. (Canceled)

21. (Currently amended) A method for protecting valued content comprising the steps of:

electronically acquiring by a provider a digital string from a purchaser to form an acquired digital string, said acquired digital string having a latent value at least to said purchaser;

modifying said acquired digital string in at least two different manners to form at least two different modified digital strings;

embedding said at least two different modified digital strings in a preexisting digital file to form an embedded digital file, said preexisting digital file having independent value to said provider;

embedding in said embedded digital file a provider digital string announcing a reward for detecting that said embedded digital file has been illicitly distributed to other than said purchaser; and

conveying said embedded digital file, as valued content, to said purchaser.

22. (Previously presented) A method in accordance with the method of claim 21, wherein said modifying step comprises encrypting said acquired digital string using at least two different encryption keys.

23. (Previously presented) A method in accordance with the method of claim 22, wherein said encrypting step further comprises the step of encrypting said acquired digital string with a public encryption key of a private/public encryption key pair forming a private digital string.

24. (Previously presented) A method in accordance with the method of claim 22, wherein said encrypting step further comprises the step of encrypting said acquired digital string with a private encryption key of a private/public encryption key pair forming a public digital string.

25. (Previously presented) A method in accordance with the method of claim 21, wherein said embedding step further comprising the step of generating a digital watermark from said at

least two different modified digital strings.

26. (Canceled)

27. (Currently amended) A method in accordance with the method of claim ~~26~~21, further comprising the step of encrypting said provider digital string.

28-30. (Canceled).

31. (Original) A method in accordance with the method of claim 21, wherein said embedding step further comprises embedding said acquired digital string in a digitized image.

32. (Original) A method in accordance with the method of claim 21, wherein said embedding step further comprises embedding said acquired digital string in digitized audio.

33. (Original) A method in accordance with the method of claim 21, wherein said embedding step further comprises embedding said acquired digital string in a video image.

34. (Original) A method in accordance with the method of claim 21, wherein said acquiring step further comprises acquiring information from said purchaser that places said purchaser at increased financial risk when known by another.

35. (Canceled)

36. (Previously presented) A method for a provider to protect valued content comprising the steps of:

electronically acquiring a digital string from a purchaser, said acquired digital string

having a latent value at least to said purchaser;

encrypting said acquired digital string according to at least one first encryption key to form a corresponding at least one encrypted digital string;

embedding said at least one encrypted digital string in a decryption key;

embedding said acquired digital string two or more times in a preexisting digital file having independent value to a content owner to form an embedded digital file, wherein said acquired digital string is embedded at least once in a hidden manner;

encrypting said embedded digital file according to a second encryption key to form an encrypted digital file;

conveying said decryption key and said encrypted digital file, as valued content, to said purchaser; and

said provider conveying to the public a published one of said at least one first encryption key, the published encryption key usable to recover in clear form said acquired digital string from said decryption key.

37. (Currently amended) A system for generating valued content in a digital form by a provider, comprising:

a processor;

a storage device coupled to said processor;

an interface coupled to said processor and to a purchaser system; and

a valued content in a digital form comprising:

a preexisting digital file having independent value to a content owner, and

a digital string provided by a purchaser in clear form to said processor, said digital string having a latent value at least to said purchaser, modified according to a key and embedded two or more times in said preexisting digital file by said processor to form a second digital file to be conveyed to said purchaser system as valued content using said interface, wherein said provider makes said key publicly available, and wherein said embedded digital string is

extractable in clear form from said second digital file using ~~only~~ said key.

38-41. (Canceled)

42. (Original) The system of claim 37, further comprising a point of sale machine coupled to said processor.

43. (Previously presented) The system of claim 42, further comprising:

a sale interface coupled to said point of sale machine; and

a network connection coupled to said interface and to said sale interface.

44. (Currently amended) A system for generating valued content in a digital form comprising:

a purchaser processor adapted to communicate to a provider system an interest in purchasing a preexisting digital file from a content owner, said preexisting digital file having independent value to said content owner;

an interface coupled to said purchaser processor and said provider system, said provider system adapted to request a purchaser digital string from said purchaser processor, said purchaser digital string having a latent value at least to a purchaser;

a storage device coupled to said purchaser processor and adapted to send said purchaser digital string to said provider processor using said interface, wherein said provider system adds to said purchaser digital string a notice of a reward, modifies said purchaser digital string to form at least two different modified digital strings, and embeds said at least two different modified digital strings at least once each into said preexisting digital file to form a modified digital file, wherein the reward is for detecting that said modified digital file has been illicitly distributed to other than said purchaser.

45-46. (Canceled)

47. (Previously presented) A processor readable medium in accordance with claim 2, wherein said hidden digital string is a plurality of hidden digital strings each encrypted according to a different key.

48. (Previously presented) A processor readable medium in accordance with claim 1, wherein said modified digital string is a plurality of modified digital strings each modified according to a different key.

49. (Currently amended) A method in accordance with the method of claim ~~21~~22, wherein at least one of the encryption keys is made publicly available by said provider.

50. (Currently amended) A method in accordance with the method of claim 49, wherein said embedded digital file is processable by a computer program using ~~only~~ a single one of said publicly available encryption keys to reveal said digital string as provided by said purchaser.

51. (Currently amended) A method in accordance with the method of claim ~~49~~50, wherein said computer program, or a process performable by said computer program to reveal said digital string, is made publicly available by said provider.

52. (Previously presented) A method in accordance with the method of claim 49, wherein fewer than all of the encryption keys are made publicly available by said provider.

53. (Previously presented) A method in accordance with the method of claim 49, wherein said provider informs said purchaser that said at least one of the encryption keys is made publicly available.

54. (Currently amended) A method in accordance with the method of claim ~~49~~53, wherein said purchaser is informed by said provider during the purchase of said valued content by said purchaser.

55. (Currently amended) A method in accordance with the method of claim ~~21~~22, wherein at least one of the encryption keys is made publicly available by said provider at a first time, and wherein at least another one of the encryption keys is made publicly available by said provider at a second time later than the first time.

56. (Currently amended) A method in accordance with the method of claim ~~21~~25, wherein a process performable by a computer program to extract said digital string in clear form from said digital watermark is made publicly available by said provider.

57. (Canceled)

58. (Currently amended) A method in accordance with the method of claim 36, comprising:

conveying to the public a computer program configured to recover said acquired digital string in clear form from ~~only~~ said decryption key ~~and~~ using said published first encryption key and without using said any additional key.

59. (Previously presented) The system of claim 44, wherein each of said at least two different modified digital strings is formed by said provider system encrypting said purchaser digital string using a different encryption key.

60. (Currently amended) The system of claim 59, wherein the provider system makes at

least one of the encryption keys publicly available, and wherein said modified digital file is processable by a computer program using ~~only~~ a single one of the publicly available encryption keys to reveal said purchaser digital string in clear form.

61. (Previously presented) The system of claim 44, wherein at least one of the at least two different modified digital strings is embedded a plurality of times into said preexisting digital file.

62. (Currently amended) A processor readable medium encoded with data representing a valued content and having a data structure comprising:

a preexisting digital file having independent value to a provider of said valued content;

two or more encoded digital strings embedded in said preexisting digital file by a provider system, each encoded digital string generated using a key from an unencoded digital string provided by a purchaser to said provider system, said unencoded digital string having a latent value to at least said purchaser of said valued content;

wherein said key is made publicly available by said provider, and wherein said valued content is processable by a computer program using ~~only~~ said key to reveal said unencoded digital string.

63. (Currently amended) The processor readable medium of claim 62, wherein at least ~~some~~ one of said two or more encoded digital strings are generated from said unencoded digital string using different keys.

64. (New) A method for protecting valued content comprising the steps of:

electronically acquiring by a provider a digital string from a purchaser to form an acquired digital string, said acquired digital string having a latent value at least to said purchaser;

modifying said acquired digital string in at least two different manners to form at least

two different modified digital strings;

embedding said at least two different modified digital strings in a preexisting digital file to form an embedded digital file, said preexisting digital file having independent value to said provider;

embedding in said embedded digital file a provider digital string having information supplied by a provider; and

after embedding said modified digital strings and said provider digital string, conveying said embedded digital file, as valued content, to said purchaser.

65. (New) A processor readable medium in accordance with claim 1, wherein said embedded digital file on said processor readable medium is processable by said computer program using said key but no additional key to reveal said embedded digital string in clear form.

66. (New) A processor readable medium in accordance with claim 1, wherein said embedded digital file on said processor readable medium is not processable by said computer program using said key to reveal said preexisting digital file in clear form.

67. (New) The system of claim 37, wherein said embedded digital string is extractable in clear form from said second digital file using said key but no additional key.

68. (New) The system of claim 37, wherein said preexisting digital file is not extractable in clear form from said second digital file using said key.

69. (New) The processor readable medium of claim 62, wherein said valued content is processable by said computer program using said key but no additional key to reveal said unencoded digital string.

70. (New) A method in accordance with the method of claim 36, wherein said published encryption key is usable to recover in clear form said acquired digital string from said decryption key without using any additional key.